UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

LAUREN SHEMELYA, on behalf of herself and all others similarly situated, Plaintiff, v. RECEIVABLES PERFORMANCE MANAGEMENT, LLC Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Lauren Shemelya ("Plaintiff") brings this Class Action Complaint against Receivables Performance Management, LLC ("RPM" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and safeguard personal identifiable information ("PII")[1] of Plaintiff and Class Members, including, but not limited to, Social Security numbers.

2. According to Defendant's website, Defendant is "a national leader in accounts receivable management."[2]

3. Prior to and through April 8, 2021, Defendant obtained the PII of Plaintiff and Class Members, and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network.

4. On or before May 12, 2021, Defendant learned of a data breach on its network that occurred on or around April 8, 2021 (the "Data Breach").

5. Defendant determined that, during the Data Breach, an unknown actor may have accessed and/or acquired the PII of Plaintiff and Class Members.

6. On or around November 21, 2022, Defendant began notifying various states Attorneys General of the Data Breach.

7. On or around November 21, 2022, Defendant began notifying Plaintiff and Class Members of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that may have been accessed and/or acquired by an unauthorized actor included

[1] Personally identifiable information generally includes information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. *See* 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *See* http://www.receivablesperformance.com/ (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Social Security numbers.

9. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

10. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited more than a year after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully kept secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

11. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention of, detection of, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Lauren Shemelya is a citizen of North Carolina residing in Winston Salem, North Carolina.

16. Defendant is a Washington limited liability company with a principal place of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

business in Lynnwood, Washington.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

20. Defendant is a citizen of Washington because it is a limited liability company formed under Washington law, its principal place of business is in Lynnwood, Washington, and its members are Howard George, a citizen of Washington, and BreAnna Stockdale, a citizen of Washington.

21. The Western District of Washington has personal jurisdiction over Defendant because it conducts substantial business in Washington and this District.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

IV. FACTUAL ALLEGATIONS

Background

23. Defendant, a debt collector, collected the PII of Plaintiff and Class Members from its customers and/or from alleged creditors of Plaintiff and Class Members that assigned their purported debts to Defendant.

24. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

26. On or about November 21, 2022, Defendant sent Plaintiff and Class Members a *Notice of Data Breach*. Defendant informed Plaintiff and other Class Members that:

> **What Happened?** On or about May 12, 2021, RPM became aware of a data security incident that impacted its server infrastructure and took our systems offline. RPM responded immediately by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.
>
> **What Information Was Involved?** The forensic investigation determined that first access to RPM's systems occurred on approximately April 8, 2021, with the ransomware launched on May 12, 2021. While the findings of the forensic investigation were not

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> conclusive, the data security incident may have resulted in unauthorized access to and/or acquisition of certain data on RPM's systems. As a result, in an abundance of caution, RPM began undertaking extensive efforts to gather and review this data to identify the presence of any personal information.
>
> RPM began this process by identifying and collecting all data that may have been accessed or acquired in connection with the data security incident. Given the complexities of RPM's server infrastructure, these efforts were extensive. RPM thereafter undertook a comprehensive, time intensive data review process, including manual review, of these documents to identify the presence of any personal information. This process concluded on or around October 2, 2022. Through this review process, RPM identified the presence of your personal information in the files that were reviewed, including Social Security number. **Please note that it is entirely possible that your specific personal information was not impacted as a result of the incident.** RPM also obtained confirmation to the best of its ability that the information is no longer in the possession of the third party(ies) associated with this incident.
>
> **What We Are Doing.** As stated above, RPM responded immediately to the data security incident by physically disconnecting all equipment and began undertaking necessary efforts to restore its systems. Immediately following the incident and over a 36-hour time frame, RPM rebuilt its shared servers from the ground up and removed and re-installed all collection and dialing software on all equipment. RPM also retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised. Please be advised that RPM is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.[3]

27. Defendant admitted in the *Notice of Data Breach* that an unauthorized actor accessed sensitive information about Plaintiff and Class Members, including Social Security numbers.

[3] Exhibit 1 (sample Notice of Data Breach filed with Maine Attorney General).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

28. In response to the Data Breach, Defendant claims that it is "continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future."[4] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

29. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

30. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

31. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

32. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

33. In October 2019, the Federal Bureau of Investigation published online an article

[4] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[5]

34. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[6]

35. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

36. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of

[5] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Nov. 28, 2022).

[6] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Nov. 28, 2022).

[7] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

37. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of that PII, and Defendant's type of business had cause to be particularly on guard against such an attack.

38. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

39. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

40. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

41. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to Plaintiff and Class Members, and it knew or should have known that it was responsible for protecting their PII from disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

43. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[8]

44. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 28, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[9]

45. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it. . . .

[9] *Id.* at 3–4.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .[10]

46. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use

[10] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[11]

47. Given that Defendant was storing the PII of more than 3.7 million individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

48. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of more than 3.7 million individuals, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

49. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to

[11] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

maintain or stored data in an Internet-accessible environment only when there was a reasonable need to do so.

50. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

51. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

53. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

54. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity

[12] 17 C.F.R. § 248.201 (2013).

[13] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches for prices ranging from $900 to $4,500.[16]

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17]

57. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Nov. 28, 2022).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Nov. 28, 2022).

[16] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Nov. 28, 2020).

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at* https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

58. The fraudulent activity resulting from the Data Breach may not come to light for years.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

61. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it stored, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

---

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Nov. 28, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

63. To date, Defendant has offered Plaintiff and Class Members only one year of credit monitoring and identity theft detection through Equifax. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

64. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

65. Plaintiff received Defendant's *Notice of Data Breach*, dated November 21, 2022, on or about that date. The notice stated that Plaintiff's personal information, including Social Security number, may have been accessed and/or acquired by an unauthorized actor.

66. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

67. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

68. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

69. Plaintiff stores any documents containing her sensitive PII in a safe and secure

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

70. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

71. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

72. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

73. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

74. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII was compromised in the data breach that is the subject of the *Notice of Data Breach* that Defendant sent to Plaintiff and Class Members on or around November 21, 2022 (the "Nationwide Class").

75. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

76. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

77. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendant has identified millions of individuals whose PII was compromised in the Data Breach, and the Class is apparently identifiable within Defendant's records.

78. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, nominal and/or treble damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

79. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

80. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

81. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

82. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

83. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to afford relief to Plaintiff and Class Members for the wrongs alleged. Defendant would necessarily gain an unconscionable advantage in individual actions because it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

84. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

85. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

86. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

87. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

88. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, nominal and/or treble damages, and/or injunctive relief as a result of Defendant's wrongful

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

conduct.

VI. CLAIMS FOR RELIEF

COUNT I
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, RCW 19.86
(On Behalf of Plaintiff and the Nationwide Class)

89. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

90. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce.

91. Defendant is a "person" as described in RCW 19.86.010(1).

92. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

93. In the course of conducting its business, Defendant committed "unfair acts or practices" by, among other things, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

94. Defendant's conduct was also deceptive. Defendant failed to timely notify and instead concealed from Plaintiff and Class Members the unauthorized release and disclosure of their Private Information. If Plaintiff and Class Members had been notified in an appropriate

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information and identities.

95. Defendant's above-described unfair or deceptive acts or practices in violation of the CPA affects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

96. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

97. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff and Class Members' business and property. Plaintiff and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, among other things, (1) an imminent, immediate and continuing increased risk of identity theft and fraud; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; (6) the financial and temporal cost of credit monitoring, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them.

98. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks an injunction prohibiting Defendant from continuing such wrongful conduct, requiring Defendant to modify its corporate culture, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect PII.

99. Plaintiff, on behalf of herself and the Class Members, also seeks to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff, on behalf of Plaintiff and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

COUNT II
NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

100. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

101. Defendant has full knowledge of the sensitivity of the PII it stored and stores, as well as the types of harm that Plaintiff and the Nationwide Class could and would suffer if that PII were wrongfully disclosed.

102. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

103. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

104. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

105. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

106. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiff's and the Nationwide Class's confidential PII in the course of its debt collection practices.

107. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

108. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

109. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

110. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

111. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

112. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

113. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

114. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

115. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

116. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the time the PII was within Defendant's possession or control.

117. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

119. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

120. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

121. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

122. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

123. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how its PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention of, detection of, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

124. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

125. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Declaratory Judgment

(On Behalf of Plaintiff and the Nationwide Class)

127. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 88.

128. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

129. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of her PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

130. Plaintiff and Class Members have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiff's

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and Class Members' PII, including Social Security numbers, while storing that PII in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including Plaintiff's Social Security number.

131. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiff and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Class harm.

132. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal, industry, and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

133. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and she will be forced to bring multiple lawsuits to rectify the same conduct.

134. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

135. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, statutory, nominal, and treble damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: November 28, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
s/ Kaleigh N. Boyd
Jason T. Dennett, WSBA #30686
Kaleigh N. Boyd, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
kboyd@tousley.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications forthcoming*